U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Cybersecure Interconnection of Distributed Energy Resources

Cybersecure integration of Distributed Energy Resources into the power grid

Background

Utilities use state-of-the-art tools for reliable integration of Distributed Energy Resources (DER) within the power grid. These tools evaluate how power grid operations might be affected by various DER integration scenarios, and help the utility develop strategies to ensure reliability and safety of the power grid. These tools were developed in response to rapid wide-scale DER deployment, and are now in common use to aid the process of operating a grid with high penetration of DER. As power system technologies continually advance, these tools must also be advanced to assist the development of cyber-secure architectures for the new communication and control pathways that are being introduced with technologies such as smart inverters and local storage control.

Objectives

Develop a tool that can evaluate the cybersecurity risk of various DER integration architectures, and design remediation strategies so that a grid with high-penetration of DER can become more resilient and better able to survive a cyber-attack.

Enable industry to cost-effectively utilize these tools in the interconnection process.

Project Description

This project will research, develop and demonstrate a co-simulation tool to evaluate and analyze the risk posed by various interconnection architectures for DER communications and control pathways. It will also assist with the design of mitigation strategies to reduce the risk that a cyber-attack might disrupt power systems that benefit from high penetration of DER. The tool will streamline analysis approaches for utilities and product vendors to use best practices for cybersecurity protection during interconnection, without increasing cost or time to interconnect. Several strategies for mitigation will be developed and demonstrated, for instance diversification of communication protocols, as one example.

Benefits

- Project will provide proactive, accurate and defensible strategies for cyber secure DER integration
- Utility and vendor interaction will allow rapid transition of research results for use by the energy sector
- Coupling of power grid and cyber expertise with physical hardware gives full range of potential scenarios and solutions
- Product will enable rapid simulation without increased cost or time to interconnect at utility & customer level

Partners

- Lawrence Livermore National Laboratory (LLNL)
- Hawaiian Electric Utility (HECO)
- Revolutionary Security
- Eaton
- SolarEdge
- OSISoft
- Power Standards Laboratory (PSL)
- Smarter Grid Solutions (SGS)
- Riverside Public Utilities

Period of Performance

October 2017 – September 2019

Total Project Cost

$2,500,000

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) research and development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber-attacks.

Contact Information:

Carol Hawk
Program Manager
DOE OE
202-586-3247
carol.hawk@hq.doe.gov

Emma M. Stewart
Principal Investigator
Lawrence Livermore National Laboratory
925-422-1902
stewart78@llnl.gov

For More Information:

http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity

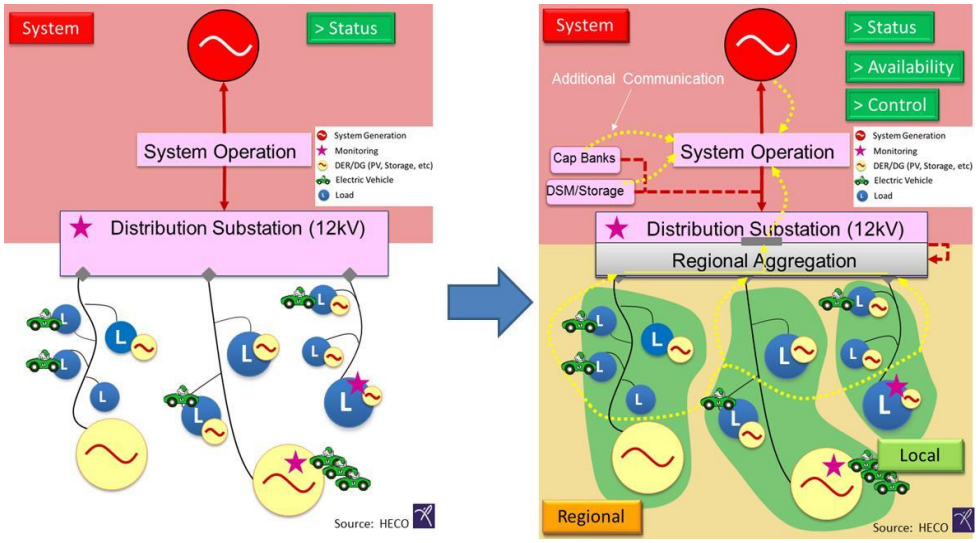

Figure 1: Integration of Distributed Resources and new communication and control framework will require cross network analysis and understanding

Technical Approach

Utilize co-simulation tools for distribution, communication and integration of new DER, for both evaluation of cyber-hosting capacity, remediation and interconnection, develop interface for rapid multi-scenario analysis. Develop a multi-phased approach for developing, applying and transitioning the tool to the energy sector over a two-year period, addressing key bulk power system and distribution-level grid architecture scenarios.

Phase 1: Tool Design and Scenario Analysis

- Task 1: Develop and implement simulation and analytics tool, working with commercial simulation product vendors
- Task 2: Select cyber-attack scenarios and review with utility and vendor participants, and working groups
- Task 3: Utility data collection and evaluation, hardware testing, response, and latency characterization for simulation
- Task 4: Scenario analysis and large scale system analysis. Review results with utility and vendor participants, iteration and reporting

Phase 2: Remediation and Protection Strategy Design

- Task 1: From selected most impactful scenarios in Phase 1, determine with vendor input most effective remediation pathways, considering both power grid protection and control equipment as well as communications
- Task 2: Simulate from hardware characterization, attack, and remediation pathways
- Task 3: Benefits assessment and reporting, visualization
- Task 4: Tool commercialization and testing with working groups for technology transition

Phase 3: Commercialization and Implementation

- Task 1: Vendor integration of research product into tool
- Task 2: Reporting and benefits assessment
- Task 3: Publication and conference presentation

End Results

Project results will include the following:

- Improved fundamental understanding of cybersecurity risk and mitigation strategies for industry and utilities for the high penetration of DER
- Workshop/report on scenarios and evaluation of cyber-resilience strategy, online tool for cyber interconnection available to utility partner
- Cyber interconnection analysis product for utilization in DER community
- Publication of key results
- Strategies that consider both the power system and the computational platforms and communication pathways used to manage, monitor, protect and control the power system, to mitigate the impact that a cyber-attack might otherwise have on the local distribution level and bulk power system
- Best practice guidelines for cyber interconnection of DER